UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 09/916,606 | 07/26/2001 | Chengi Jimmy Kuo | NAI1P019/01.096.01 | 8718 |

28875 7590 01/03/2005

Zilka-Kotab, PC
P.O. BOX 721120
SAN JOSE, CA 95172-1120

| EXAMINER | |
|---|---|
| SCHUBERT, KEVIN R | |
| **ART UNIT** | **PAPER NUMBER** |
| 2137 | |

DATE MAILED: 01/03/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

| Offic Action Summary | Application No. | Applicant(s) | |
|---|---|---|---|
| | 09/916,606 | KUO ET AL. | |
| | Examiner | Art Unit | |
| | Kevin Schubert | 2137 | |

*-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --*

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

1)☒ Responsive to communication(s) filed on *26 July 2001*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

4)☒ Claim(s) *1-52* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-52* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

**Application Papers**

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *26 July 2001* is/are: a)☐ accepted or b)☒ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *09042001*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

## DETAILED ACTION

Claims 1-52 have been considered.

### *Drawings*

The drawings are objected to because of the following minor informality: the word "Parmaters" is a misspelled version of "Parameters" in Figure 6. Corrected drawing sheets in compliance with 37 CFR 1.121(d) are required in reply to the Office action to avoid abandonment of the application. Any amended replacement drawing sheet should include all of the figures appearing on the immediate prior version of the sheet, even if only one figure is being amended. The figure or figure number of an amended drawing should not be labeled as "amended." If a drawing figure is to be canceled, the appropriate figure must be removed from the replacement sheet, and where necessary, the remaining figures must be renumbered and appropriate changes made to the brief description of the several views of the drawings for consistency. Additional replacement sheets may be necessary to show the renumbering of the remaining figures. The replacement sheet(s) should be labeled "Replacement Sheet" in the page header (as per 37 CFR 1.84(c)) so as not to obstruct any portion of the drawing figures. If the changes are not accepted by the examiner, the applicant will be notified and informed of any required corrective action in the next Office action. The objection to the drawings will not be held in abeyance.

### *Claim Rejections - 35 USC § 102*

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 1-7,10,15-18,20,24-31,34,39-42,44, and 50 are rejected under 35 U.S.C. 102(e) as being anticipated by Muttik, U.S. Patent No. 6,775,780.

As per claims 1,24, and 50, the applicant discloses a method for protecting a computer comprising the following limitations which are met by Muttik:

a) running a computer on a network in an opened share mode (Col 3, lines 30-42; Fig 1);

b) monitoring attempts to access the computer by applications utilizing the network (Col 1, lines 66-67; Col 2, lines 1-11; Fig 1);

c) determining whether the applications attempt to modify the computer (Col 2, lines 9-11; Fig 2);

d) executing a security event in response to any attempt to modify the computer (Col 2, lines 12-15; Col 2, lines 31-36; Fig 2);

The disclosed invention provides a method for preventing virus infiltration in a network where computers exchange data by monitoring access of applications attempting to modify the computer in a virtual world and executing a security event in response to a malicious attempt to modify the computer. Similarly, the primary reference discloses a security method for protecting a computer on a network from viruses by running the applications received from the network through an emulator and analyzing them to determine whether they are malicious.

Regarding part a), a remote host can send data, which can access data stored in the computer, across a network (Fig 1).

Regarding part b), since the computer is in an opened share mode in which data coming from the network can access data stored the computer, the computer emulates the code in a virtual space in order to monitor for malicious behavior (Fig 1).

Regarding part c), a determination step occurs as to whether the code is OK or malicious (Fig 2).

Regarding part d), the security event can be a number of things depending on which embodiment of the primary reference is used. In one embodiment, the security event is notifying the user (Fig 2). In another embodiment, the analysis of the software is terminated (Col 2, lines 31-36). Since the software

or application must pass through the emulator in order to be legitimately executed by the computer system, the software or application is never executed in real space.

Regarding claims 24 and 50, since the implementation of the system takes place in a computing system, the use of computer code and logic is met.

As per claims 2 and 26, the applicant discloses the method of claims 1 and 24, which are met by Muttik (see above), with the following limitation which is also met by Muttik:

Wherein the opened share mode allows other computers on the network to access data stored on the computer (Col 3, lines 30-42);

As per claims 3 and 27, the applicant discloses the method of claims 1 and 24, which are met by Muttik (see above), with the following limitation which is also met by Muttik:

Wherein the opened share mode includes a virtual opened share mode (Col 2, lines 2-5; Fig 2);

As can be seen by the lines referenced above and throughout the primary reference, the applications coming off the network are put in a virtual mode through the use of the emulator. Also, the applications have no knowledge they will be put through an emulator.

As per claims 4 and 28, the applicant discloses the method of claims 3 and 27, which are met by Muttik (see above), with the following limitation which is also met by Muttik:

Wherein the virtual opened share mode indicates to other computers of an ability to write to the computer (Col 2, lines 2-5; Col 5, lines 10-11);

The applications coming from the network are placed in an insulated environment to monitor their system calls for malicious behavior (Col 2, lines 2-5). Furthermore, one system call that may be deemed malicious behavior is a system call to write an executable file with a particular name (Col 5, lines 10-11).

As per claims 5-7 and 29-31, the applicant discloses the method of claims 4-5 and 28-29 respectively, which are met by Muttik (see above), with the following limitation which is also met by Muttik:

Wherein the computer operates in the virtual opened share mode by modifying an application program interface (Col 4, lines 32-41);

The computer modifies an application program interface and operates in a virtual world where application program interface (API) calls are recorded to see if malicious activity is taking place. Regarding claims 6,7,30, and 31, the primary reference discloses the general use of monitoring application program interface calls. As is known in the art, the application program interface includes an operating system program interface and a network application program interface.

As per claims 10 and 34, the applicant discloses the method of claims 1 and 24, which are met by Muttik (see above), with the following limitation which is also met by Muttik:

Wherein the opened share mode applies to each of a plurality of networks of which the computer is a member (Col 3, lines 37-42; Fig 1);

The applicant should note the network (102 in Fig 1) can include a "combination of networks" (Col 3, lines 40-41).

As per claims 15 and 39, the applicant discloses the method of claims 1 and 24 respectively, which are met by Muttik (see above), with the following limitation which is also met by Muttik:

Wherein any attempt to modify the computer is utilized in a heuristic analysis for identifying a coordinated attack on multiple computers (Col 1, lines 66-67; Col 2, lines 1-11);

The applicant should note that the emulator records a pattern of system calls and analyzes the behavior of the application which can be viral in a heuristic analysis type approach. The rules (210 of Fig 2) can be set to a plurality of preferences, including determination of a coordinated attack.

As per claims 16 and 40, the applicant discloses the method of claims 1 and 24 respectively, which are met by Muttik (see above), with the following limitation which is also met by Muttik:

Wherein attempts to modify the computer are tracked (Col 3, lines 66-67; Col 4, lines 1-11; Fig 2);

As illustrated in Fig 2 and the lines referenced above, system calls are tracked and then fed into a comparator for determination of malicious behavior.

As per claims 17-18 and 41-42, the applicant discloses the method of claims 1 and 24 respectively, which are met by Muttik (see above), with the following limitation which is also met by Muttik:

Wherein it is determined whether the applications attempt to write to memory in the computer, and the security event is executed in response to any attempt to write to memory in the computer (Col 5, lines 10-11);

As described above, attempting to write a file with a particular name to memory is one example of a rule that can be set to determine malicious behavior. If the user desires, any attempt to write to memory could be deemed malicious behavior. Regarding claims 18 and 42, this includes any attempt to copy the virus to memory. Also, the security event can be alerting the user (Col 2, lines 12-15) or terminating analysis of the software thereby not allowing the software or application to be executed in real space (Col 2, lines 31-36). The use of either of these security events or both of these security events depends on which embodiment of the primary reference is used.

As per claims 20 and 44, the applicant discloses the method of claims 1 and 24 respectively, which are met by Muttik (see above), with the following limitation which is also met by Muttik:

Wherein the security event includes terminating the application attempting to modify the computer (Col 2, lines 31-36);

As described earlier, terminating the analysis of the software attempting to modify the computer based on a decision that the software is malicious means that the software will not be executed in real time since software coming off the network must pass the emulator test before being executed in real time.

As per claim 25, the applicant discloses the method of claim 24, which is met by Muttik (see above), with the following limitation which is also met by MuttikL

Wherein the network includes the Internet (Col 3, lines 19-21).

***Claim Rejections - 35 USC § 103***

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 8-9,11-14,32-33,35-38, and 48-49 are rejected under 35 U.S.C. 103(a) as being unpatentable over Muttik in view of Jordan, U.S. Patent Application Publication No. 2002/0073323.

As per claims 8 and 32, the applicant describes the method of claims 1 and 24, which are met by Muttik (see above), with the following limitation which is met by Jordan:

Wherein the opened share mode indicates a file structure parameter and a name parameter [0008];

Muttik discloses all the limitations of the independent claims. However, Muttik fails to disclose the use of having some resources privileged and others freely accessible to network applications.

Jordan discloses a virus detection system similar to that of Muttik's in which the computer determines in virtual space whether the applications exhibit malicious behavior based on whether they attempt to access privileged resources on a computer. Muttik, however, does disclose the use of "recording parameters of individual system calls within the pattern of system calls" (Jordan: Col 2, lines 28-30) as a further means to analyze the behavior of the applications coming off the network.

It would have been obvious to one of ordinary skill in the art at the time the invention was filed to combine the ideas of Muttik with those of Jordan and have parameters such as file structure parameters or name parameters be used to signify a set of privileged access files in the case where the user or the computer wants to designate some files as privileged.

As per claims 9 and 33, the applicant describes the method of claims 1 and 24, which are met by Muttik (see above), with the following limitation which is met by Jordan:

Wherein the opened share mode indicates a plurality of parameters that are randomly selected to prevent detection [0008];

Muttik discloses all the limitations of the independent claims. The use of parameters, such as a file structure parameter and a name parameter, is met above through Muttik in view of Jordan. The use of randomly selecting parameters by the computer to prevent detection by the application would be an obvious improvement. Since Muttik accounts for using parameters to determine whether or not applications from the network are allowed to execute (Col 2, lines 28-30) and Jordan accounts for a dichotomy of privileged access and non-privileged access system resources [0008], randomly selecting the parameters used for determining whether the applications from the network can access privileged resources would be an obvious improvement so that applications from the network cannot fool the system.

Thus, it would have been obvious to one of ordinary skill in the art at the time the invention was filed to combine the ideas of Muttik with those of Jordan as well as incorporate the obvious idea of randomly selecting parameters to test the applications from the network to prevent the computer from being fooled.

As per claims 11-14 and 35-38, the applicant limits the method of claims 1,11,24, and 35, which are met by Muttik (see above), with the following limitation which is met by Jordan:

Wherein the opened share mode applies only to a predetermined list of application programs executable on the computer [0008];

Muttik discloses all the limitations of the independent claims. However, Muttik fails to disclose the opened share mode applying only to predetermined list of application programs. Jordan teaches a virus detection system similar to Muttik's in which virus detection and protection is implemented to allow a user to access resources that aren't protected and block access to resources that are protected.

Muttik teaches that system calls are monitored by the emulator and the rules (210 in Fig 2) are used to determine whether the behavior of the applications from the network are malicious. It would have been obvious to one of ordinary skill in the art at the time the invention was filed to incorporate Jordan's use of a set of privileged access resources and a set of normal access resources into Muttik's rules section to designate which computer resources can be used by the applications from the network and which cannot.

Regarding claims 12-13 and 36-37, generating the list or set of privileged resources for the rules (210 in Fig 2) of claims 11 and 35 includes generating the list manually or automatically.

Regarding claims 14 and 38, if the system of Muttik in view of Jordan is implemented as described above, the system has a set of privileged access resources and a set of non-privileged access resources in the emulator rules section which means that the user has two different opened share modes in communication with other users or applications on the network.

As per claims 48 and 49, the applicant limits the computer program product of claim 24, which is met by Muttik (see above), with the following limitation which is met by Jordan:

Wherein at least a portion of the computer code resides on a gateway ([0029] and [0030]);

Muttik discloses all the limitations of the independent claim. However, Muttik fails to disclose the use of a gateway. Jordan describes a similar virus protection system to Muttik's in which applications are put in a virtual space before being actually run on a computer.

Jordan also describes having the apparatus and methods of the system be embodied in a transmission medium [0029]. Jordan further discloses that "the computer virus detection methodologies may be performed on a file...before the file is stored/copied/executed/opened on the computer" [0030]. A gateway is a transmission medium which connects the user to the network. Though Jordan does not explicitly use the term gateway, he does disclose the idea of using a gateway or similar device to analyze the application before it goes to the computer. Regarding claim 49 and in accordance with both Muttik and Jordan, if the file is determined to be malicious it would therefore be blocked from entering the computer. It would have been obvious to one of ordinary skill in the art at the time the invention was filed

to combine the ideas of Muttik with those of Jordan and implement the use of a gateway to block access to a computer so that files are analyzed and discarded before they even have a chance to get to the computer.

Claims 19,21-23,43,45-47,51, and 52 are rejected under 35 U.S.C. 103(a) as being unpatentable over Muttik in view of Schnurer, U.S. Patent No. 5,842,002.

As per claims 19 and 43, the applicant describes the method of claims 1 and 24, which are met by Muttik (see above), with the following limitation which is met by Schnurer:

Wherein the security event includes logging the computer off the network in response to any attempt to modify the computer (Col 8, lines 26-35);

Muttik discloses all the limitations of the independent claims. However, Muttik fails to go into detail about the actions taken when malicious code is detected. Schnurer discloses a virus trap system similar to Muttik's in which certain actions are taken when malicious code is detected. One of these actions is "shutting down a network segment" (Col 8, line 33). This includes logging a computer off the network. It would have been obvious to one of ordinary skill in the art at the time the invention was filed to combine the ideas of Muttik with those of Schnurer to further protect the computer once an application has been deemed malicious.

As per claims 21 and 45, the applicant describes the method of claims 1 and 24, which are met by Muttik (see above), with the following limitation which is met by Schnurer:

Wherein the security event includes deleting the application attempting to modify the computer (Col 8, lines 26-35);

Muttik discloses all the limitations of the independent claims. However, Muttik fails to go into detail about the actions taken when malicious code is detected. Schnurer discloses a virus trap system similar to Muttik's in which certain actions are taken when malicious code is detected. One of these actions is "deleting the file" (Col 8, line 30). It would have been obvious to one of ordinary skill in the art

at the time the invention was filed to combine the ideas of Muttik with those of Schnurer to further protect the computer once an application has been deemed malicious.

As per claims 22 and 46, the applicant describes the method of claims 1 and 24, which are met by Muttik (see above), with the following limitation which is met by Schnurer:

Wherein the security event includes an alert transmitted via the network (Col 8, lines 26-35);

Muttik discloses all the limitations of the independent claims. However, Muttik fails to go into detail about the actions taken when malicious code is detected. Schnurer discloses a virus trap system similar to Muttik's in which certain actions are taken when malicious code is detected. One of these actions is "notifying the sender and receiver of the file or program" (Col 8, lines 29-30). It would have been obvious to one of ordinary skill in the art at the time the invention was filed to combine the ideas of Muttik with those of Schnurer to further protect the computer once an application has been deemed malicious.

As per claims 23 and 47, the applicant describes the method of claims 22 and 46, which are met by Muttik (see above), with the following limitation which is met by Schnurer:

Wherein the security event includes information associated with the application attempting to modify the computer (Col 8, lines 26-35);

Muttik discloses all the limitations of the independent claims. However, Muttik fails to go into detail about the actions taken when malicious code is detected. Schnurer discloses a virus trap system similar to Muttik's in which certain actions are taken when malicious code is detected. One of these actions is "notifying the sender and receiver of the file or program" (Col 8, lines 29-30). It would have been obvious to one of ordinary skill in the art at the time the invention was filed to combine the ideas of Muttik with those of Schnurer to further protect the computer once an application has been deemed malicious.

As per claims 51 and 52, the applicant describes a method for protecting a computer in an opened share mode with the following limitations which are met by Muttik in view of Schnurer:

a) running a computer on a network in a virtual opened share mode, wherein the virtual opened share mode allows other computers on the network to access predetermined data and programs resident on the computer, and indicates to other computers of an ability to write to the computer (claims 1a,2,4);

b) monitoring attempts to access the computer by applications utilizing the network (claim 1b);

c) determining whether the applications attempt to modify the computer (claim 1c);

d) tracking the attempts of the applications to modify the computers (claim 16);

e) transmitting an alert via the network in response to any attempt to modify the computer, wherein the alert includes information associated with the applications attempting to modify the computer (claim 22);

f) logging the computer off the network in response to any attempt to modify the computer (claim 19);

g) deleting any application attempting to modify the computer (claim 21);

h) wherein any attempt to modify the computer is utilized in a heuristic analysis for identifying a coordinated attack on multiple computers (claim 15);

As one can see all the limitations of the claim are met by claims previously rejected. The applicant should note that parts a) through d) and part h) are met by Muttik, and parts e) through g) are met by Muttik in view of Schnurer.

Regarding claim 52, since the implementation of the system takes place in a computing system, the use of computer code is met.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kevin Schubert whose telephone number is (571) 272-4239. The examiner can normally be reached on M-F 8:00-5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Andrew Caldwell can be reached on (571) 272-3868. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Andrew Caldwell
Andrew Caldwell

***